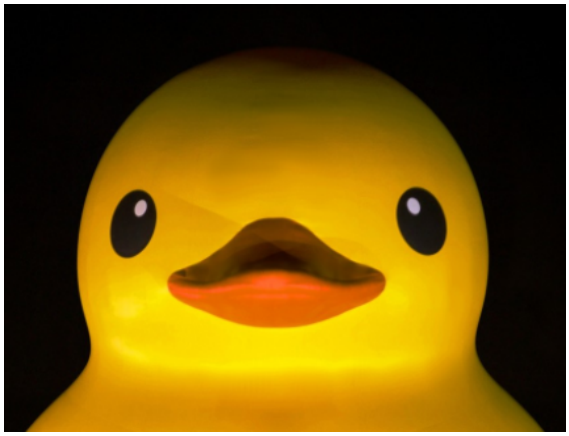
Lab 6

Rubber Ducky



Estimated time to complete: 50 Min

WHAT YOU WILL LEARN

How to create a USB rubber ducky for offensive security and automation purposes.

WHY IT'S IMPORTANT

A USB rubber ducky is a very dangerous tool for offensive security as it is a common way to inject keystrokes, steal information, or upload a payload.

SKILLS GAINED

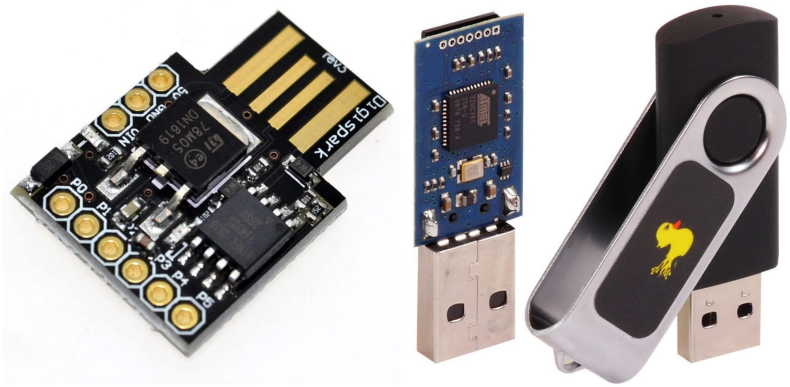
- Creating a USB rubber ducky
- Upload payloads
- Scripting for automation

REQUIRED HARDWARE

- Raspberry Pi
- Internet Connection
- Digispark USB

WHAT IS A USB RUBBER DUCKY?

A USB rubber ducky is a tool to inject various payloads into an unsuspecting computer by posing as a human interface device like a keyboard or mouse. The rubber ducky can then do anything a keyboard could and more such as run scripts, install malware, change wallpaper, establish web connections, and steal user information.



WHAT CAN YOU DO WITH A RUBBER DUCKY?

There are various premade rubber ducky payloads you can find on github, though for more serious attacks, you probably would want to create your own payload. The github repository for our specific device is located here: https://github.com/CedArctic/DigiSpark-Scripts. In this repository there are payloads for embedding keyloggers, creating windows accounts, changing wallpapers, mouse tweaks, and network listeners. On plug-in, a rubber ducky will automatically run the payload, so all you have to do is plug the ducky into a computer and it will do the rest.

Create_Account	Added hide option for created user	2 years ago
DNS Poisoner	Renamed DNSPoisoner to add .ino file extension	2 years ago
Execute_Powershell_Script	Added Talker and Powershell Script Executer	5 years ago
Fork_Bomb	Typo in README.md	2 years ago
Hi_Chewy	updated link to wav	2 years ago
Keylogger	Added Keylogger Script	2 years ago
Rapid_Shell	Update README.md	4 years ago
Reverse_Shell	Typo fix	16 months ago
RickRoll_Update	Fixed fakeupdate url for Win10	2 years ago
Silly_Mouse	Add Silly_Mouse script	2 years ago
Talker	Fixed Talker and added Wifi grabber	5 years ago
Wallpaper_Changer	Fixed a comment	5 years ago
Wallpaper_Changer_macOS	Add README	2 years ago
Wallpaper_Prank	Fixed Wallpaper_Change name, added Wallpaper_Prank	5 years ago
WiFi_Profile_Grabber	Update to Wifi_Profile_Grabber	2 years ago
WiFi_Profile_Mailer	Update WiFi_Profile_Mailer_New.ino	9 months ago
Window_Jammer	Create Window_Jammer.ino	4 years ago

WHY ARE RUBBER DUCKYS SO DANGEROUS?

A rubber ducky will begin to execute whatever is programmed onto it automatically once it's plugged in, without needing a user's permission. An attacker could use this to steal personal information on your machine before you have a chance to stop it. For this reason it is important to not plug in any random USB devices you see on the floor. If a curious employee at a company were to find a USB drive and plug it in, the entire company could suffer the loss of data and information. An attacker could "accidentally" drop a few USB rubber duckys around, and oftentimes curiosity will get the better of people and make them want to see what's on the USB. This is a form of social engineering that can turn the rubber ducky from a fun tool to a dangerous weapon.

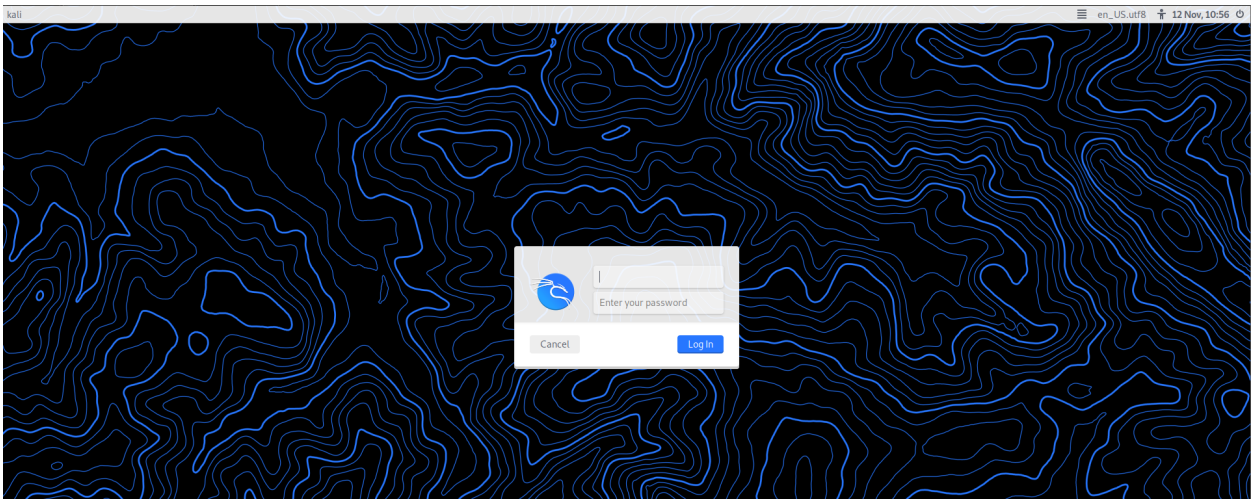
HOW TO DEFEND AGAINST A RUBBER DUCKY ATTACK?

Some host hardening should be done to prevent a rubber ducky from taking control of your computer. You should almost never be using an administrator account when using a work machine, you should instead use a normal account and provide administrator credentials when promoted. This will prevent a USB rubber ducky from running scripts on your machine without providing administrator credentials. Besides that users just need to be aware to **never** plug in an unknown flash drive, as doing so could compromise all data and hardware in the company.

GETTING STARTED WITH LINUX

STEP 1: LOG INTO KALI

To begin our journey with Linux, we must first login to our device. In order to do this, plug in your Raspberry Pi and let it boot up until you are at the login screen seen below:



Use the default login info for you H.A.C.K Device which is:

Username: HACKUser

Password: Pentesttheworld1!

Once you have done this you should be greeted to the Kali Linux Desktop as seen below

STEP 2: CONNECTING TO THE INTERNET - *DO ME PLEASE*

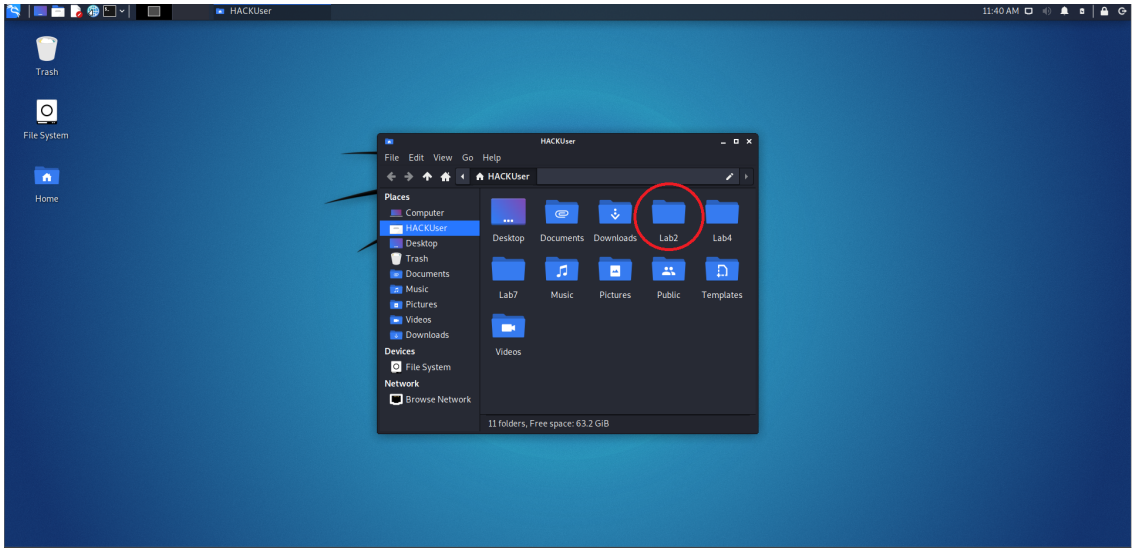
To begin, click on the network icon in the top toolbar, displayed as: 

Right click on the icon and click Enable Wi-Fi, once enabled you can click on the network icon again to see all of the available networks, click the one you would like to connect to and enter the Wi-Fi password.

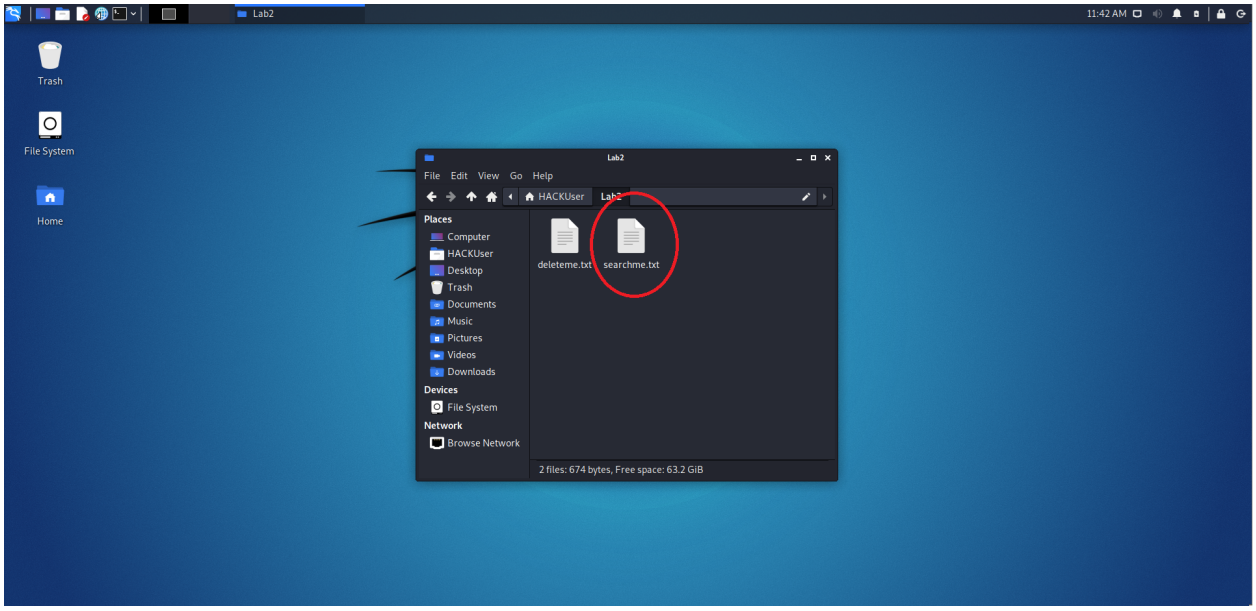
STEP 3: NAVIGATING FILES USING THE FILE BROWSER

Once we are connected to the internet, we can start learning how to navigate Linux. First, click the “Home” Icon on the Desktop

From here we can see all the files in our home directory. The home directory is the directory you find yourself in when you first log in and contains the personal files for a particular user. We can click on the Lab 2 to see the files in the folder.



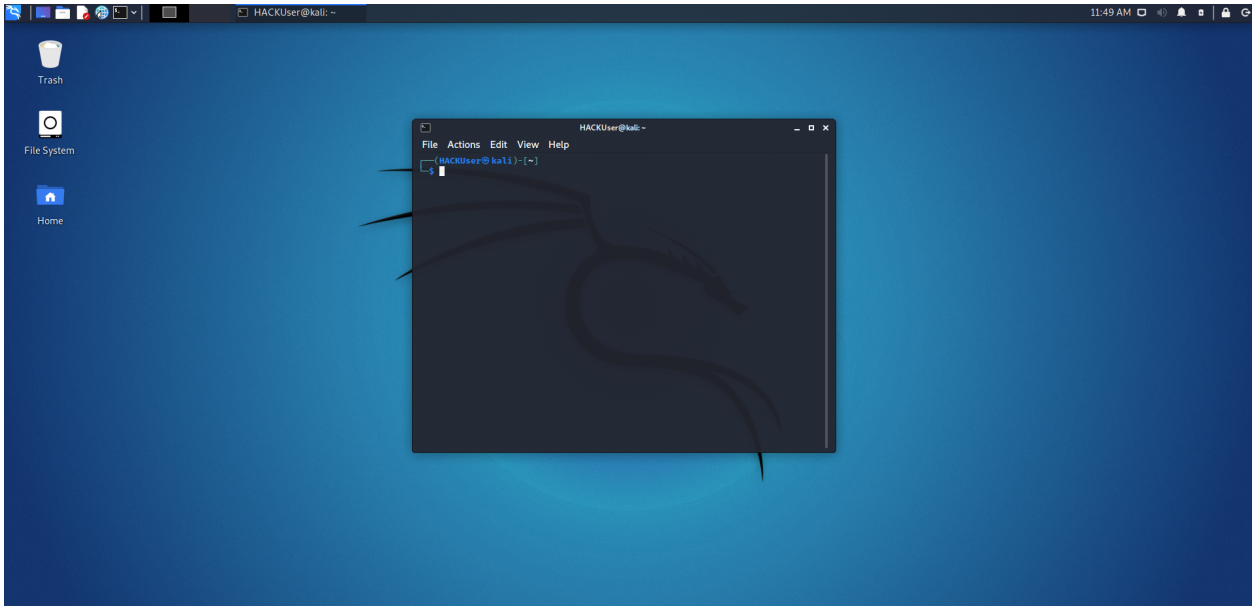
Here we should see 2 files named searchme.txt and deleteme.txt. Feel free to click on the files to see its contents



After you have inspected the contents of the file, you can begin searching around the computer using the sidebar until you feel comfortable. If you are lost and need to get back to your base home directory, you can always do **cd ~** in a terminal.

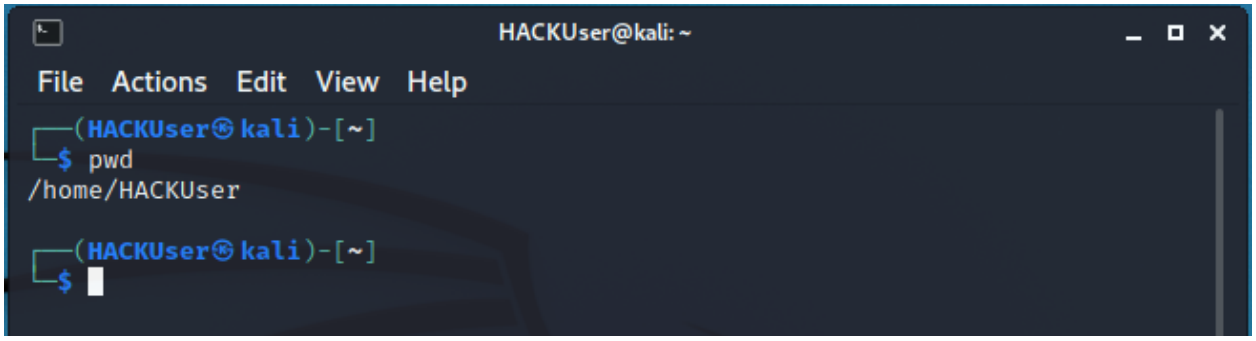
STEP 4: USING THE TERMINAL

Now that we understand what folders belong to our home directory, we can begin to learn how to use the terminal in Linux. Click the terminal icon on the top left corner in order to open a new terminal.

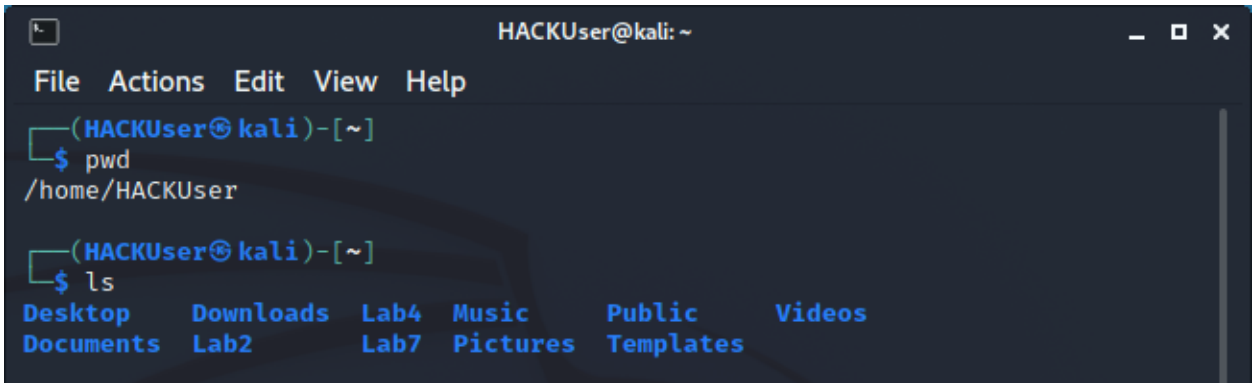


STEP 5: FINDING OUT WHERE YOU ARE - PWD AND LS

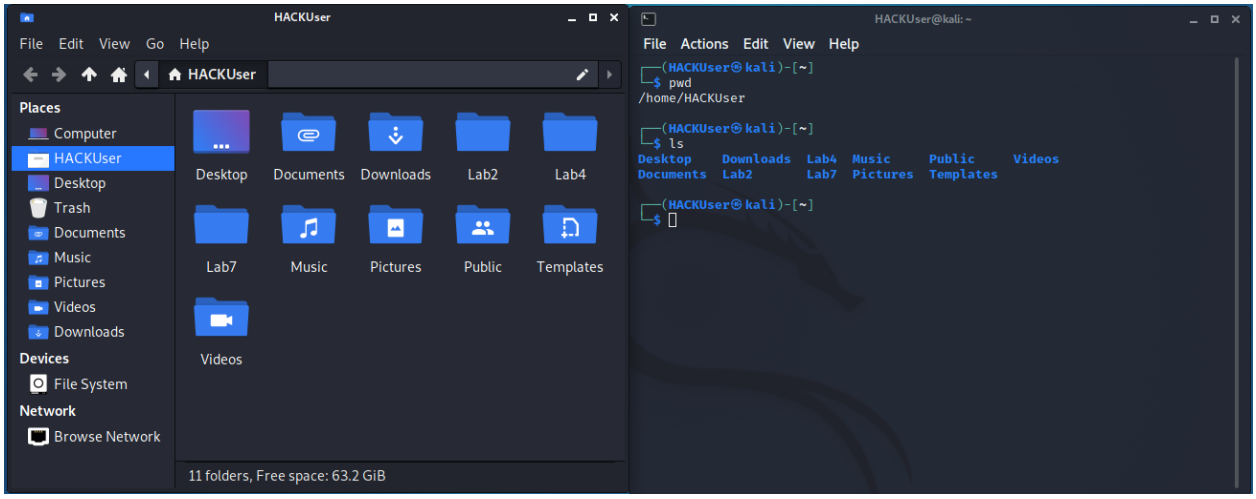
Having the terminal allows us to execute certain linux commands. However, before we begin creating items, we must find out where we are in the computer. In order to find out where we are we can type the command “pwd” and hit enter.



Here we can see that when we are at the same location that we started at when we clicked the “Home” Icon on the desktop. This is our home directory. Now that we know where we are, we can begin to see what files are in our home directory. To do this, type in the command “ls” and hit enter.

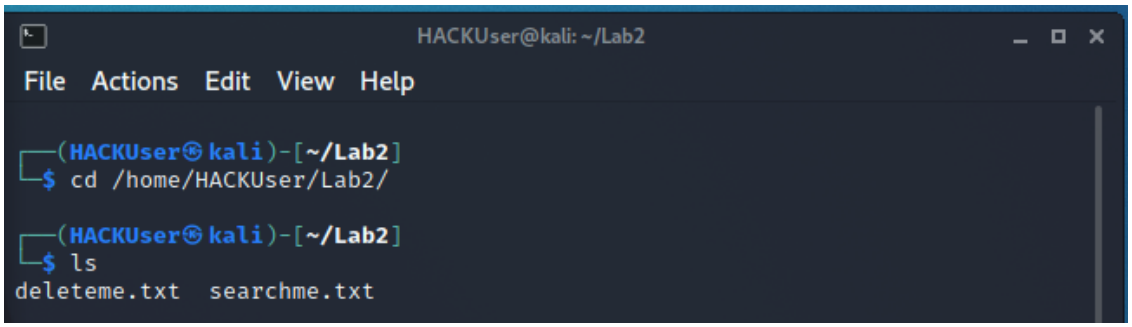


Once again, we see all the files in our home directory, we can verify this by clicking the “Home” icon on the desktop again and see that all the files are the same.



STEP 6: CHANGING WHERE YOU ARE AT - CD

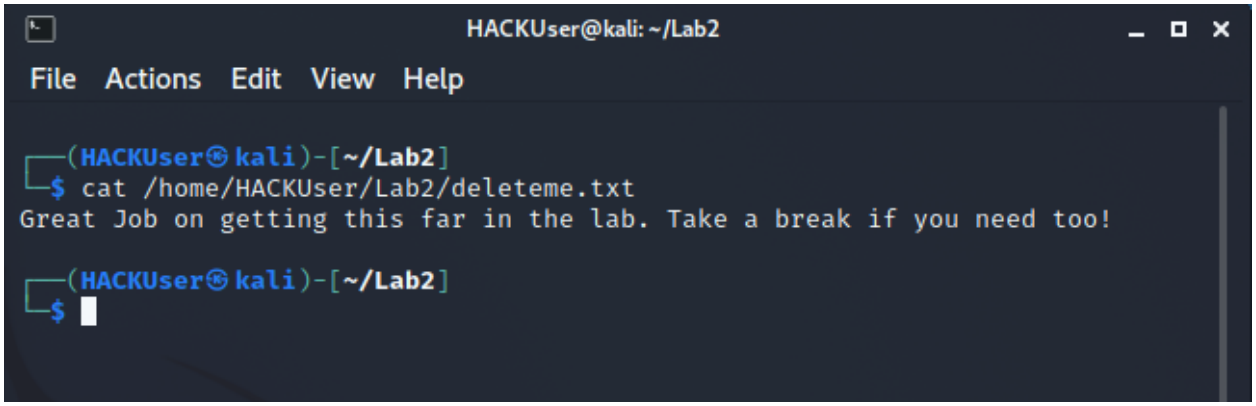
If we want to change where we are at in the terminal we can use the command "**cd**". Type the command "**cd /home/HACKUser/Lab2/**" and hit enter to change into the Lab 2 folder in your home directory. Once you've done this, use the command "**ls**" again to verify that you see the two files "deleteme.txt" and "searchme.txt"



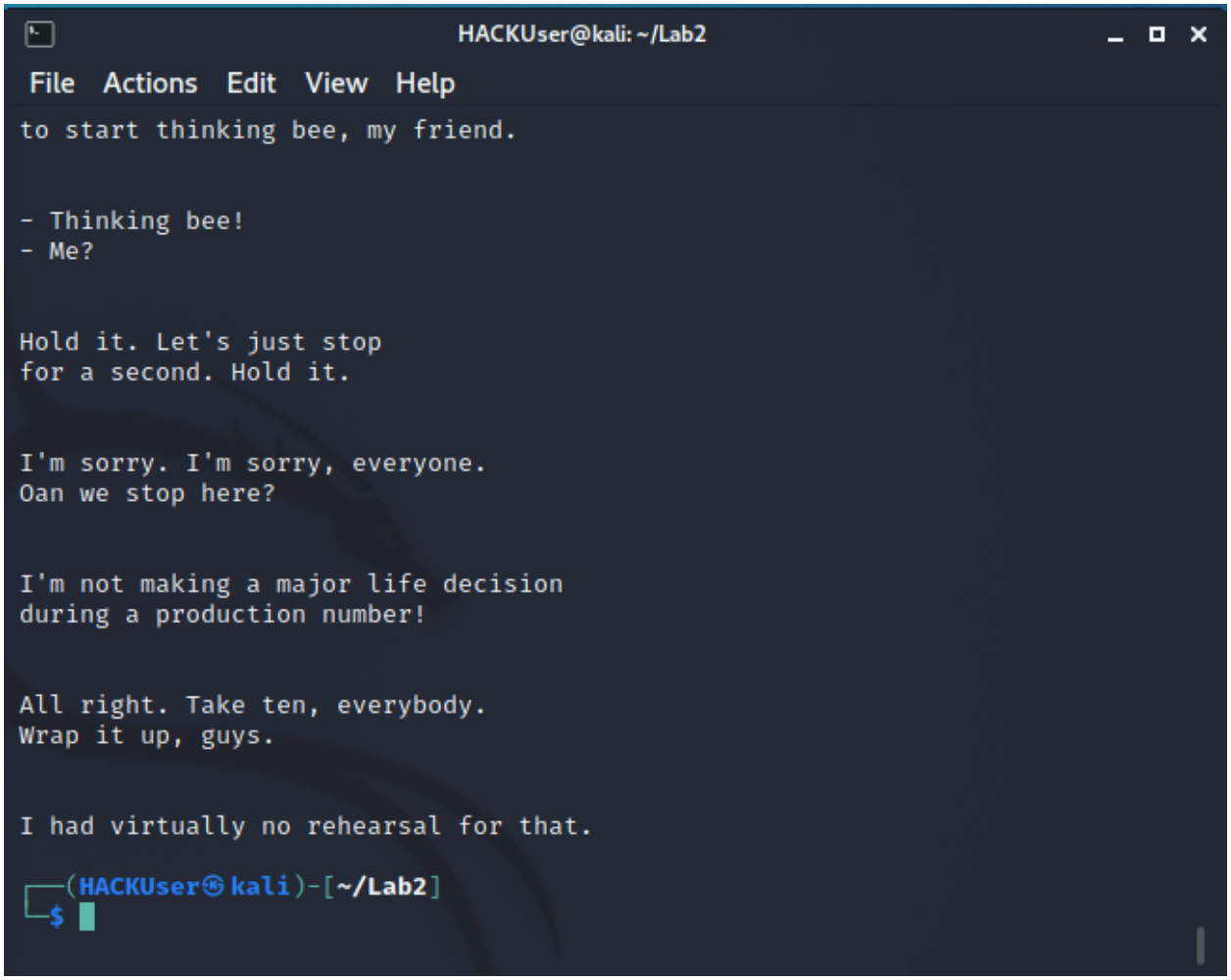
STEP 7: READING A TEXT FILE - GREP AND CAT

While seeing the files in a directory is useful, sometimes we want to see the information stored within those files. In order to view ***all*** the information in a file we can use the command

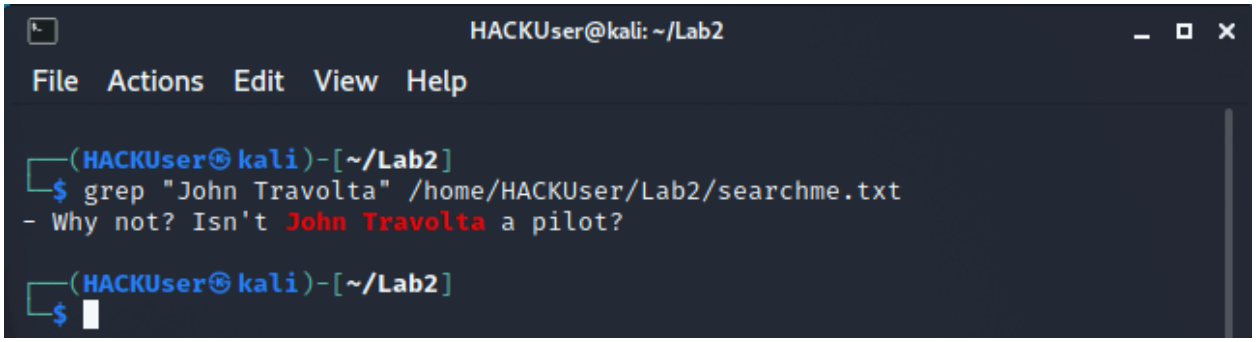
"cat". This will print out all the text to the command line. Try it out by using the command "**cat /home/HACKUser/Lab2/deleteme.txt**"



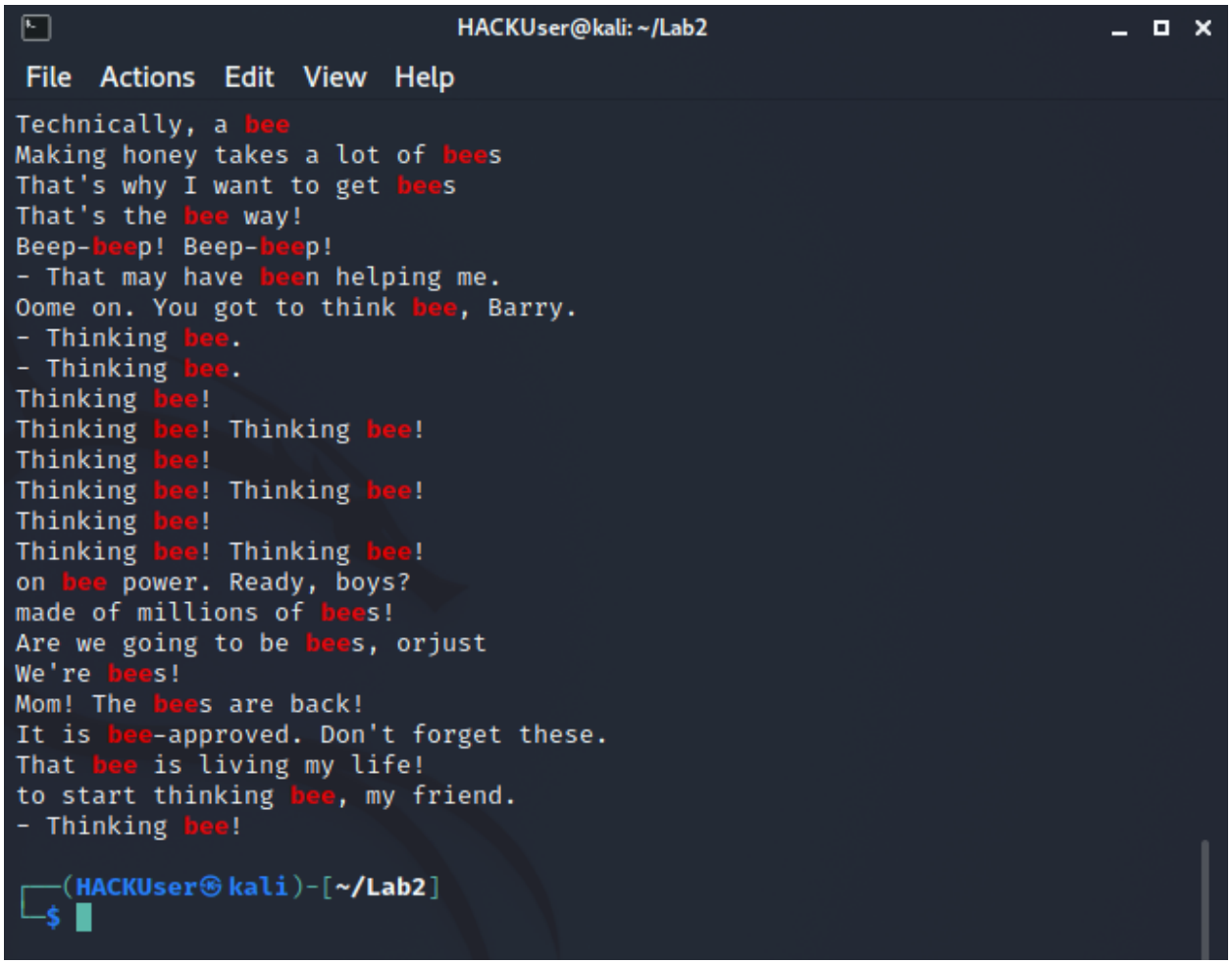
Here we can see that the file contained a short easy to read message. This is a perfect use for cat, because there isn't too much information. However, if we try to read the contents of a large file, the information can be too much for our terminal to read it all. Try to use the command "**cat /home/HACKUser/Lab2/searchme.txt**".



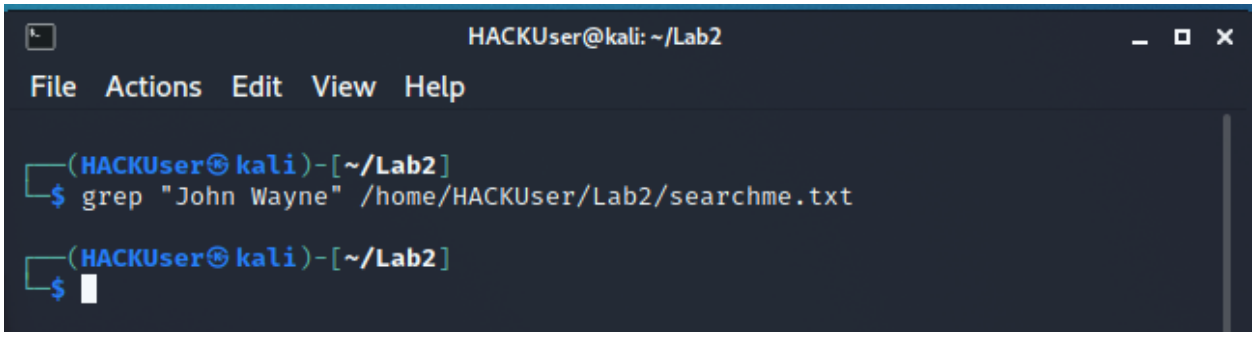
Here we can see that the file is the entire script of the Bee Movie. Our terminal doesn't display all of the info on the file and we have to scroll up to try and read the file's contents. This is where the command "grep" comes in handy. We can use it to search the contents of a file to find a specific word. For example, if we wanted to see if John Travolta was mentioned in the file, we can use the command: ***grep "John Travolta" /home/HACKUser/Lab2/searchme.txt*** . Make sure to use quotations around the word "John Travolta"



With our command we can see that John Travolta is actually mentioned in the file. We can also see how many times a certain word is in a file. Use the command ***grep "bee" /home/HACKUser/Lab2/searchme.txt*** to see how many times the word bee is mentioned in the script.



If a word is not contained within a file, grep will just return nothing. Use the command ***grep "John Wayne" /home/HACKUser/Lab2/searchme.txt*** to see if John Wayne is mentioned in the script.



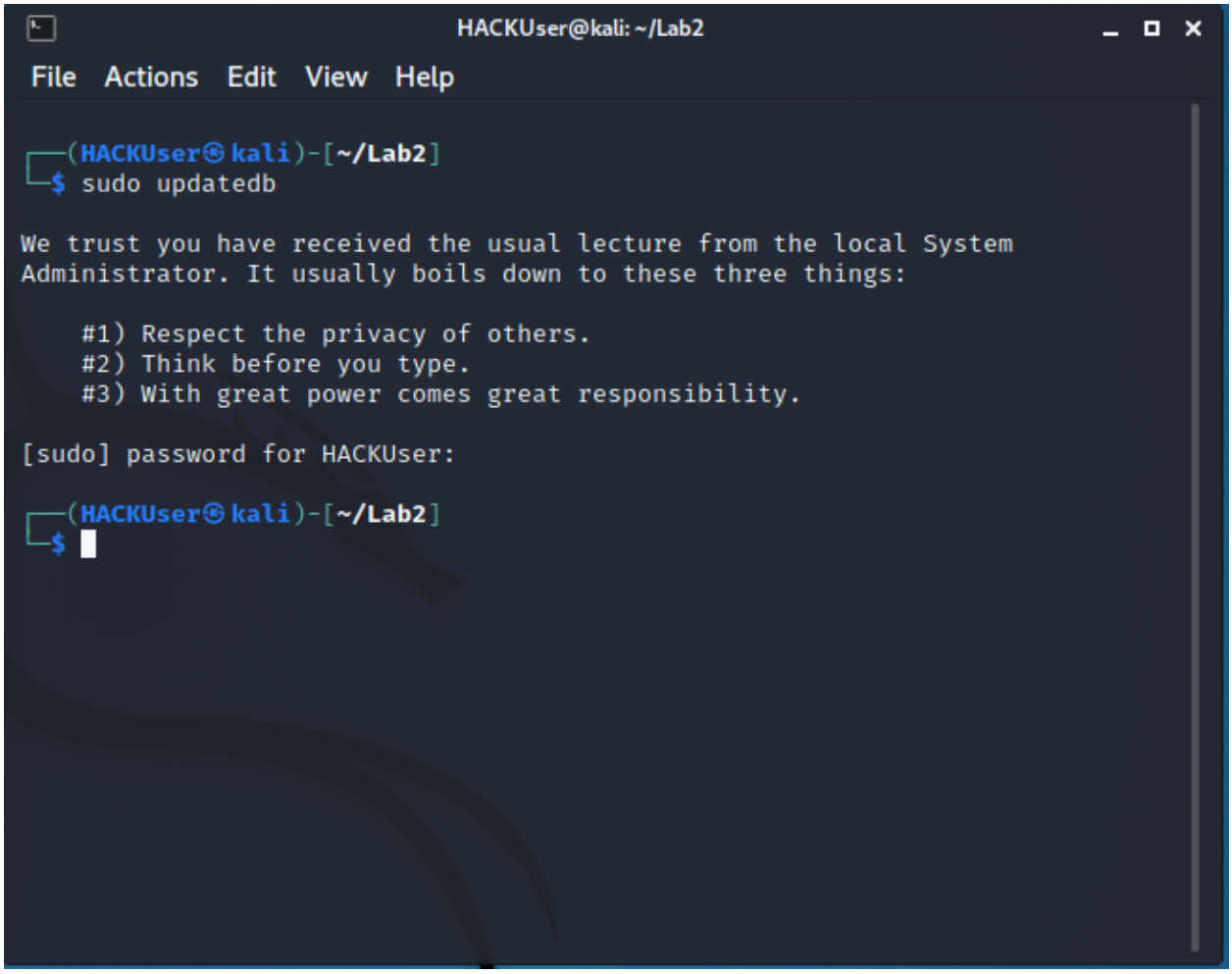
Here we can see that the words “John Wayne” are not in the file as grep returns nothing in response:

STOP: THIS IS A GOOD TIME TO TAKE A BREAK AND CONTINUE ANOTHER TIME IF NEEDED. CONSIDER THIS THE END OF PART 1 OF THE LAB.

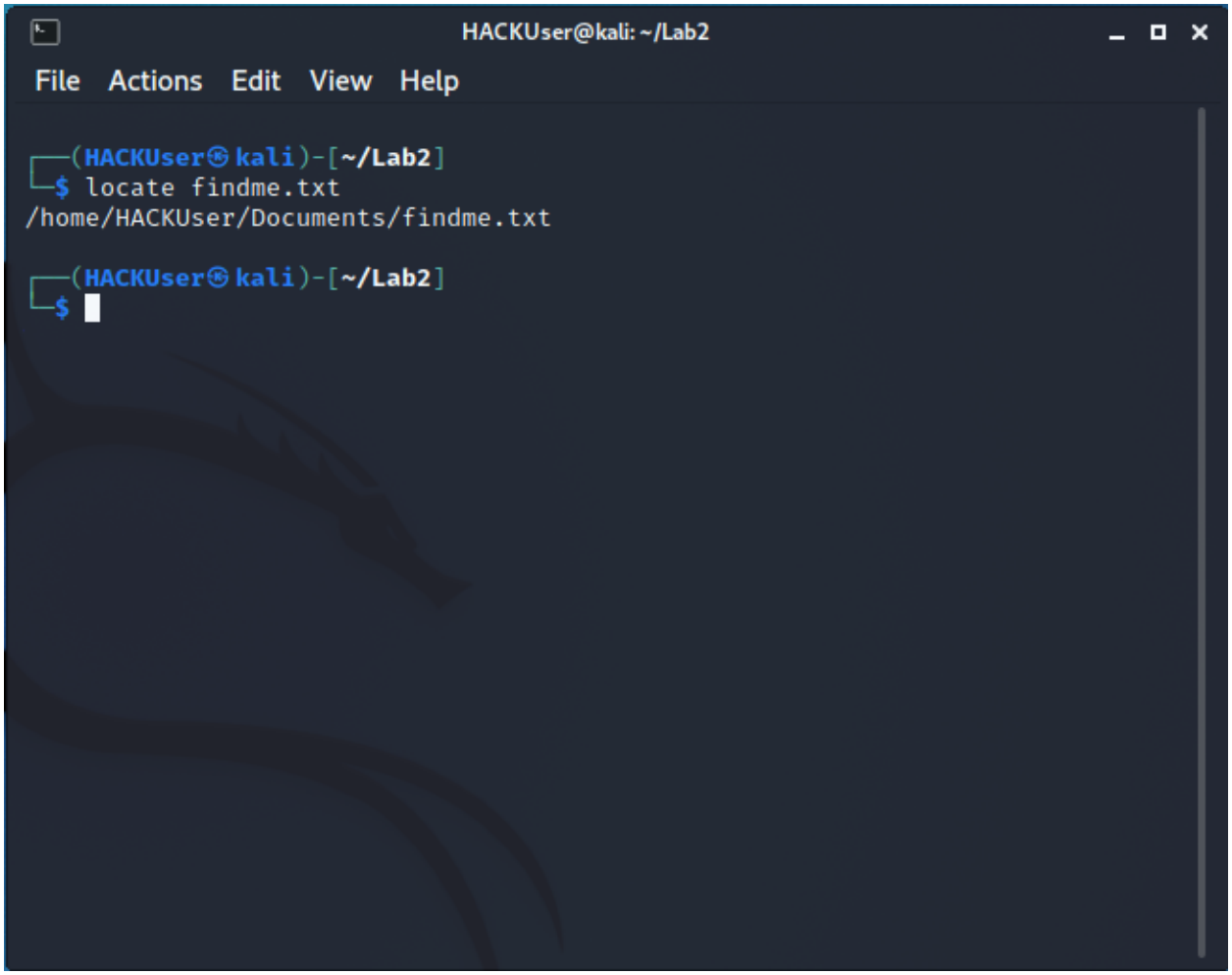
MORE WITH LINUX

STEP 8: FINDING A FILE

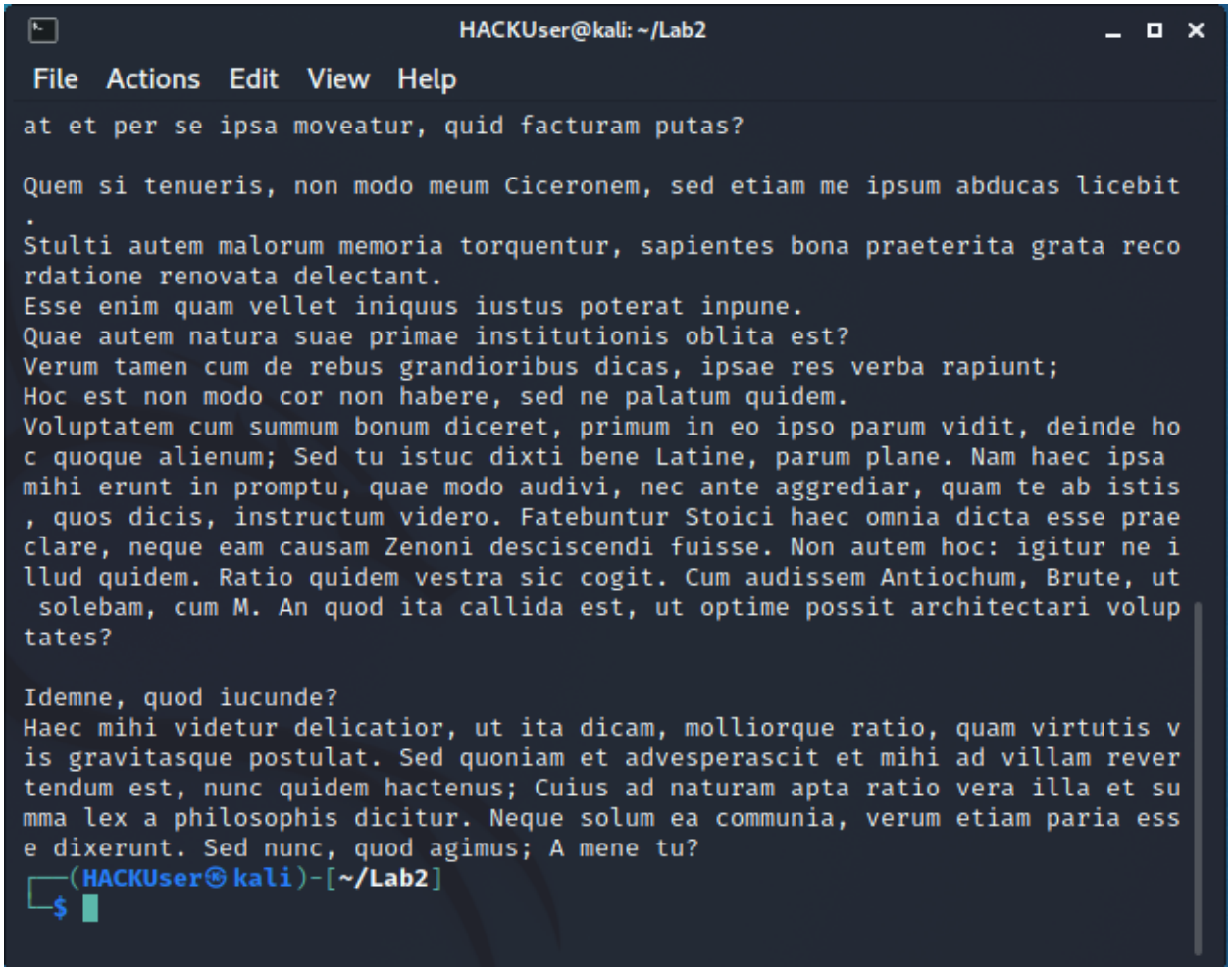
Using files is great, but sometimes you just need to find a file. In Windows, you use the start button and search bar to find files. In Linux, you will use the command “locate”. We want to find the file named findme.txt . Before we start using the locate command, first type the command “sudo updatedb” in the command line. This command makes Linux search through all the files on the system to know where they are at. Type this command in the terminal and press enter. The terminal will ask for your password, input your password “Pentesttheworld1!” and hit enter.



Now that Linux knows where all the files are on the system, type the command “locate findme.txt



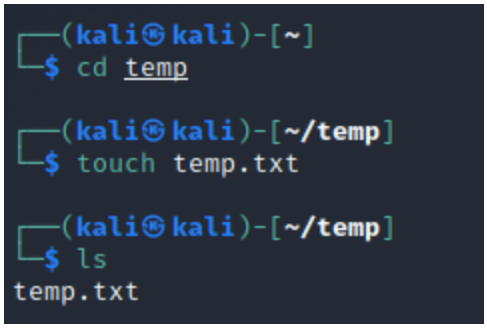
Linux tells us that the file is at /home/HACKUser/Documents/findme.txt . We can confirm this and see the content of the files using the command “cat /home/HACKUser/Documents/findme.txt”



STEP 9: MAKING FILES AND DIRECTORIES - MKDIR AND TOUCH

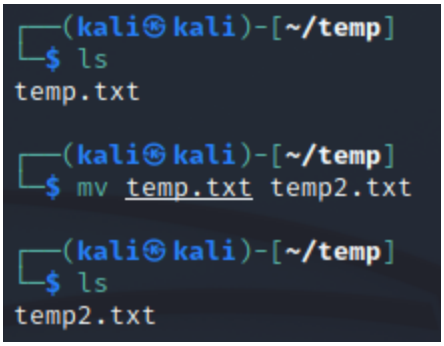
Just like in other operating systems, the Linux file system is made up of files and folders. To create a file, use the **touch** command and to make a folder, use **mkdir**. Make a folder in your home directory by doing **mkdir temp**.

Cd into the temp folder you just created and do **touch temp.txt**, you can then do **ls** to ensure the file was created correctly.



STEP 10: MOVING AND REMOVING FILES - RM AND MV

We can also rename, move and delete files with the command line as well. To rename a file, do **mv filename newname**. Try to change the name of your temp file to temp2.txt by doing **mv temp.txt temp2.txt**.



We use the mv command to move files as well, just do **mv filename /home/newlocation**. Try to move the temp2.txt file to your desktop by doing **mv temp2.txt /home/kali/Desktop**, the file should appear on your desktop.

To delete a file, just use the rm command. Delete the temp2.txt file by doing **rm temp2.txt**.

STEP 11: GETTING HELP WITH COMMANDS

To find information about or options for our command we can look at the manual page by doing **man x**. Let's do this with the ls command to start. Running **man ls** in the terminal will send you to this page:

Here you can see how to use the command under synopsis, a description of what the command does and the options you can use with the command. You can also see author and version info and where to send bug reports for the utility. Below you can see the difference of using **ls** and using ls with the **-all** option on the home directory.

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  DHCPig  Documents  Downloads  Lab7  Music  Pict

┌──(kali㉿kali)-[~]
└─$ ls -a
.               .bashrc.original  DHCPig      .face.icon
..              .BurpSuite        .dmrc       .gnupg
.bash_history   .cache            Documents   .ICEauthorit
.bash_logout    .config           Downloads   .java
.bashrc         Desktop           .face       Lab7
```

HOW TO USE TEXT EDITORS

There are many options to edit text files in Linux, some come pre installed but you can get more beginner friendly options with apt-get. Let's start by creating a text file on our Desktop. Enter the command **cd /home/kali/Desktop** to move to the Desktop, then do **touch test.txt** to make an empty text file, it should appear on your desktop.

Now let's install some text editors so you can see which one you like. You can download notepadqq or leafpad with the command **sudo apt-get install leafpad** or **sudo apt-get install notepadqq**, these are generally easier to use than the pre-installed utilities.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install leafpad
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Suggested packages:
  evince-gtk
The following NEW packages will be installed:
  leafpad
0 upgraded, 1 newly installed, 0 to remove and 537 not upgraded.
Need to get 90.9 kB of archives.
After this operation, 465 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 1s (81.9 kB/s)
Selecting previously unselected package leafpad.
(Reading database ... 277766 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
Processing triggers for kali-menu (2021.3.3) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for mailcap (3.70) ...
```

Now you can open the text file by using the name of the text editor then the file name, such as **leafpad text.txt**. This will open the file and allow you to edit it. Other utilities preinstalled to do this are **vi**, **vim**, **gedit**, and **nano**. Which one you use is personal preference.

Try using a few of these utilities and see which one you like best.

REVIEW

1: What are common uses of Linux?

A) Supercomputers

B) Smart devices

C) Desktops

D) All of the above

2: The mkfile command is used to create a new empty file (True/False)

3: Which cd command will take you to your home directory?

A) cd ~

B) cd .

C) cd -

D) cd home

4: What Linux command is used to find information about another command?

A) help

B) man

C) info

D) guide

5: The most common way to install a software or tool on Linux is using a package manager (True/False)

6: Which statement about Linux is **NOT** true?

A) Linux is open source

B) There are many different versions of Linux

C) Linux command line is barely used

D) Linux can run on almost any hardware

Answers: 1:D 2:False 3:A 4:B 5:True 6:C